

| NODIS Library | Legal Policies(2000s) | Search |



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May
16, 2006
Expiration Date: May
16, 2011

[Printable Format \(PDF\)](#)

[Request Notification of Change](#) (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) |
[Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) | [Chapter11](#) |
[Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) | [Chapter16](#) | [Chapter17](#) |
[Chapter18](#) | [Chapter19](#) | [Chapter20](#) | [Chapter21](#) | [AppendixA](#) | [AppendixB](#) |
[ALL](#) |

Chapter 6 Information and Information System IT Security Strategy

6.1. In the development of an SSP, the information and information system owner shall document the information and information system strategy. A system strategy provides a high-level description of how the system operates, which includes a high-level design schematic of the system and corresponding security characteristics of the system such as types of data, user communities, interconnectivity, and data flows (i.e., who and how users will interact with the information, how information will move between locations and users) and the desired information management goals and objectives.

6.2 Information security covers not just information but all infrastructure that facilitates its use such as processes, systems, services, technology, etc., and including computers, voice, and data networks. NASA is required to develop an IT security strategy in the initiation phase for each system that lays out the end-to-end IT security, which is defined as "safeguarding information from point of origin to point of destination." The vision is that security needs to possess an end-to-end property, otherwise security breaches are possible at the interfaces, which can result in building gaps. This type of strategy can significantly streamline the design process since it supports a variety of resource-specific considerations early on in the system's IT security life cycle. By establishing and maintaining a unifying vision and strategic direction, the information system owner can ensure that through each phase of the IT security life cycle that the protection of the information and information system is being met. This means that the

information system owner needs to refer continually back to the IT security strategy as the system moves through the IT security life cycle to ensure that the strategy is being implemented and that the strategy itself is still valid.

6.3 No one can ever eradicate all risk of improper or capricious use of any information. The level of information security sought in any particular situation should be commensurate with the value of the information and the loss, financial or otherwise, that might accrue from improper use (i.e., disclosure, degradation, denial, etc.). The strategy should capture these choices.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) |
[Chapter5](#) | [Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) |
[Chapter11](#) | [Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) |
[Chapter16](#) | [Chapter17](#) | [Chapter18](#) | [Chapter19](#) | [Chapter20](#) |
[Chapter21](#) | [AppendixA](#) | [AppendixB](#) | [ALL](#) |

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
